Art Unit: 2135

DETAILED ACTION

1. Claims 10, 12-17, and 21-35 are pending.

EXAMINER'S AMENDMENT

An examiner's amendment to the record appears below. Should the changes and/or additions be unacceptable to applicant, an amendment may be filed as provided by 37 CFR 1.312. To ensure consideration of such an amendment, it MUST be submitted no later than the payment of the issue fee.

Authorization for this examiner's amendment was given in a telephone interview with Catherine Voorhees on 5/6/2008.

The application has been amended as follows:

29. (Currently Amended) A secret reconstruction system for carrying out a secret reconstruction method for reconstructing a secret in a secret sharing scheme that generates n first shares from the secret information, n being an integer equal to or greater than two, the n shares being distributed to a group having n members in such a way that the original secret information can be reconstructed by a collection of any t members ($2 \leq t \leq n$), the secret reconstruction system comprising: a plurality of shared secret reconstruction apparatuses, ~~as deseribed in claim 10~~ wherein each shared secret reconstruction apparatus for reconstructing a secret, used for a case where n first shares are generated from original secret information, n being an integer equal to or greater than two, by using a first threshold secret sharing scheme, in which the original secret information can be reconstructed by a collection of at least any k members from a group having n members ($2 \leq t \leq n$), and the n shares are distributed to the n members, t members collected from the n members separately possessing the shared secret reconstruction apparatus, t being an integer equal to or greater than k, the shared secret reconstruction apparatus thus operating together with t - 1 other shared secret reconstruction apparatuses, the shared secret reconstruction apparatus comprising:
a secret sharing operation unit, when t members are collected from the n members, generating second shares from a first share held by the shared secret reconstruction apparatus by using a (t, t) threshold secret sharing scheme, in which original secret information can be reconstructed by a collection of t members from the collected t members, and distributing the second shares to the t shared secret reconstruction apparatuses of the collected t members including itself; and a secret reconstruction operation unit calculating an intermediate result for reconstructing the original secret

information in a distributed computation by use of the output from the secret sharing operation unit and the second shares received from the t - 1 other shared secret reconstruction apparatuses and transmitting the intermediate result; wherein the secret sharing operation unit generates third shares from member ID held by the shared secret reconstruction apparatus bv using a secret sharing scheme and distributes them to the t - 1 other shared secret reconstruction apparatuses, the secret reconstruction operation unit thereby calculating an intermediate result for the secret reconstruction in the distributed computation by use of the second and third shares output from the secret sharing operation unit and received from the t - 1 other shared secret reconstruction apparatuses;

wherein the secret reconstruction operation unit comprises: a term calculation unit performing a distributed multiplication on the result of a distributed computation performed on a coefficient calculated from the third share to the second share and on this second share by use of the second and third shares output from the secret sharing operation unit and received from the t - 1 other shared secret reconstruction apparatuses; and

an adder summing all the outputs from the term calculation unit; and wherein the term calculation unit comprises: a difference operation unit calculating differences between the different third

shares;

a first multiple term distributed multiplication unit performing a distributed multiplication on the outputs from the difference operation unit;

a distributed inverse element calculation unit performing a distributed computation on

the inverse element of the output from the first multiple term distributed multiplication unit; a second multiple term distributed multiplication unit performing a distributed multiplication on the third shares; and

a pair of two term distributed multiplication units performing a distributed multiplication on the output from the distributed inverse element calculation unit, the output from the second multiple term distributed multiplication unit and the corresponding second share; and

a secret reconstruction apparatus reconstructing the original secret information from the outputs of the plurality of shared secret reconstruction apparatuses.

Art Unit: 2135

Allowable Subject Matter

1. Claims 10, 12-17, and 21-35 are allowed.

2. The following is an examiner's statement of reasons for allowance: The prior art teaches A shared secret reconstruction apparatus for reconstructing a secret, used for a case where n first shares are generated from original secret information, n being an integer equal to or than 2, by using a first threshold secret sharing scheme, in which the original secret information can be reconstructed by a collection of at least any k members from a group having n members, and the n shares are distributed to the n members, t members collected from the n members separately possessing the shared secret reconstruction apparatus, t being an integer equal to or greater than k, the shared secret reconstruction apparatus thus operating together with t-1 other shared reconstruction apparatuses, the shared secret, a secret sharing operation unit, when t members are collected from the n members, generating second shares from a first share held by the shared secret reconstruction apparatus by using a (t,t) threshold secret sharing scheme, in which original secret information can be reconstructed by a collection of t members from the collected t members, and distributing them to the t shared secret reconstruction apparatuses of the collected t members including itself; a secret reconstruction operation unit calculating an intermediate result for reconstructing the original secret information in a distributed computation by use of the output from the secret sharing operation unit and the second shares received from the t-

1 other shared secret reconstruction apparatuses and transmitting the intermediate result.

The prior art fails to teach the details of wherein the secret sharing operation unit generates third shares from member ID held by the shared secret reconstruction apparatus by using a secret sharing scheme and distributes them to the t - 1 other shared secret reconstruction apparatuses, the secret reconstruction operation unit thereby calculating an intermediate result for the secret reconstruction in the distributed computation by use of the second and third shares output from the secret sharing operation unit and received from the t - 1 other shared secret reconstruction apparatuses; wherein the secret reconstruction operation unit comprises: a term calculation unit performing a distributed multiplication on the result of a distributed computation performed on a coefficient calculated from the third share to the second share and on this second share by use of the second and third shares output from the secret sharing operation unit and received from the t - 1 other shared secret reconstruction apparatuses; and an adder summing all the outputs from the term calculation unit; and wherein the term calculation unit comprises: a difference operation unit calculating differences between the different third shares;
a first multiple term distributed multiplication unit performing a distributed multiplication on the outputs from the difference operation unit; a distributed inverse element calculation unit performing a distributed computation on the inverse element of the output from the first multiple term distributed multiplication unit; a second multiple term distributed multiplication unit performing a distributed multiplication on the third shares; and a pair of two term distributed multiplication units performing a

distributed multiplication on the output from the distributed inverse element calculation unit, the output from the second multiple term distributed multiplication unit and the corresponding second share.

Any comments considered necessary by applicant must be submitted no later than the payment of the issue fee and, to avoid processing delays, should preferably accompany the issue fee. Such submissions should be clearly labeled "Comments on Statement of Reasons for Allowance."

Conclusion

Any inquiry concerning this communication or earlier communications from the examiner should be directed to RANDAL D. MORAN whose telephone number is (571)270-1255. The examiner can normally be reached on M-F: 7:00 - 4:00.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Kim Vu can be reached on 571-272-3859. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

Art Unit: 2135

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free). If you would like assistance from a USPTO Customer Service Representative or access to the automated information system, call 800-786-9199 (IN USA OR CANADA) or 571-272-1000.

/Thanhnga B. Truong/
Primary Examiner, Art Unit 2135

/R. D. M./
Examiner, Art Unit 2135

5/6/2008